IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

LATRINA COTHRON, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	
	)	**Case No. 1:19-cv-00382**
v.	)	
	)	**Honorable John J. Tharp Jr.**
WHITE CASTLE SYSTEM, INC. d/b/a WHITE CASTLE,	)	
Defendant.	)	

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff Latrina Cothron ("Plaintiff" or "Cothron") individually and on behalf of all others similarly situated (the "Class"), by and through her attorneys, brings the following Second Amended Class Action Complaint ("Complaint") pursuant to Rule 23 of the Federal Rules of Civil Procedure against White Castle System, Inc. d/b/a White Castle, ("White Castle" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Defendant White Castle System, Inc. d/b/a White Castle ("White Castle") is an Ohio corporation that owns and operates hundreds of White Castle fast-food restaurants throughout the country, including Illinois.

2. When White Castle hires an employee, he or she is enrolled in its DigitalPersona employee database, provided by Cross Match Technologies, Inc.,[1] using a scan of his or her fingerprint. White Castle uses the DigitalPersona employee database to distribute its employees' paystubs, among other things, on a weekly basis.

3. While many employers use conventional methods for payroll (direct deposit or paper check), White Castle's employees are required to have their fingerprints scanned by a biometric device to retrieve their paystubs.

4. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as White Castle – and financial institutions have incorporated biometric applications into their workplace in the form of biometric authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

5. Unlike ID badges– which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes White Castle's employees to serious and irreversible privacy risks. For example, if a database containing fingerprint data or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Google, Equifax, Uber, Home Depot, Panera, Whole Foods, Chipotle, Trump Hotels, Facebook/Cambridge Analytica, and Marriott data breaches or misuses – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

6. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million

[1] Cross Match Technologies, Inc. ("Cross Match") is a technology company that provides software and hardware that tracks and monitors employees' biometric data to companies worldwide.

federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* www.opm.gov/cybersecurity/cybersecurity-incidents.

7. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259fl38.

8. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

9. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect, store and use Illinois citizens' biometrics, such as fingerprints.

10. Notwithstanding the clear and unequivocal requirements of the law, White Castle disregards its employees' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and uses employees' biometric data in violation of BIPA. Specifically, White Castle has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose(s) and length of time for which their fingerprints were being collected, stored, and used, as required by BIPA;

b. Receive a written release from Plaintiff and others similarly situated to collect, store, or otherwise use their fingerprints, as required by BIPA;

c. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their fingerprints to a third party as required by BIPA.

11. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an Order: (1) declaring that White Castle's conduct violates BIPA; (2) requiring White Castle to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

12. Plaintiff Latrice Cothron is a natural person and a citizen of the State of Illinois.

13. Defendant White Castle is an Ohio corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

14. This Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C § 1332(d)(2)(A), (d)(5)(B) because the proposed class has 100 or more members, the amount in controversy exceeds $5,000,000.00, and the parties are minimally diverse.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to these claims occurred in this judicial district.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

16. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions,

including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

17. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

18. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

19. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

20. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or

otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;

b. Informs the subject in writing of the specific purpose(s) and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS § 14/15(b).

21. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

22. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and – most importantly here – fingerprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

23. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.*, 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

24. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS § 14/15(c)) and requires companies to develop and comply with a written policy – made available to the public – establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric

information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

25. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

26. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

II. Defendant Violates the Biometric Information Privacy Act.

27. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using individuals' biometric data stopped doing so.

28. However, Defendant failed to take note of the shift in Illinois law governing the collection, use and dissemination of biometric data. As a result, White Castle continues to collect, store, use and disseminate employees' biometric data in violation of BIPA.

29. Specifically, when employees are hired by White Castle, they are required to have their fingerprints captured and stored to enroll them in its DigitalPersona employee database(s).

30. White Castle uses an employee authentication software system supplied by Cross Match that requires employees to use their fingerprints as a means of authentication.

31. Upon information and belief, White Castle fails to inform its employees that it discloses or disclosed their fingerprint data to at least two out-of-state third-party vendors: Cross Match and DigitalPersona, and likely others; fails to inform its employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprint data.

32. Furthermore, White Castle fails to provide employees with a written, publicly available policy identifying its retention schedule and guidelines for permanently destroying employees' fingerprint data when the initial purpose for collecting or obtaining their fingerprint data is no longer relevant, as required by BIPA.

33. The Pay by Touch bankruptcy that catalyzed the passage of BIPA highlights why such conduct – where individuals are aware that they are providing biometric information but not aware to whom or for what purposes they are doing so – is dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as their fingerprints, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long. White Castle disregards these obligations, and its employees' statutory rights, and instead unlawfully collects, stores, uses and disseminates its employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

34. Upon information and belief, White Castle lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and has not and will not destroy Plaintiff's and other similarly-situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interaction with the company.

35. White Castle's employees are not told what might happen to their biometric data if and when it merges with another company or worse, if and when its business folds, or when the other third parties that have received their biometric data businesses fold.

36. Since White Castle neither publishes BIPA-mandated data retention policies nor discloses all purposes for its collection of biometric data, White Castle's employees have no idea the extent to whom it sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and the putative Class are not told to whom White Castle currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

37. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

38. By and through the actions detailed above, White Castle disregards Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Latrina Cothron's Experience

39. Plaintiff Latrina Cothron was hired by White Castle in 2004 and is currently working as a manager.

40. Approximately three years into Plaintiff's employment with White Castle, Plaintiff ***was required*** to scan and register her fingerprint(s) so White Castle could use them as an

authentication method for Plaintiff to access the computer as a manager and to access her paystubs as an hourly employee as a condition of employment with White Castle.

41. At this time, White Castle did not inform Plaintiff in writing or otherwise of the purpose(s) and length of time for which her fingerprint data was being collected, did not receive a written release from Plaintiff to collect, store or use her fingerprint data, did not provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's fingerprint data, nor did White Castle obtain Plaintiff's consent before disclosing or disseminating her biometric data to third parties.

42. White Castle subsequently stored Plaintiff's fingerprint data in its DigitalPersona employee database(s).

43. Plaintiff was required to scan her fingerprint each time she accessed a White Castle computer.

44. Plaintiff was also required to scan her fingerprint each time she accessed her paystubs.

45. It was not until October of 2018—approximately 11 years after collecting, storing, using, disclosing and disseminating her biometric data—that White Castle provided Plaintiff with an apparent "consent form".

46. Further, Plaintiff ***was required*** to scan her already registered fingerprint in order to electronically sign the apparent "consent form" provided by White Castle.

47. Plaintiff had never been informed, **prior** to the collection of her biometric identifiers and/or biometric information, of the specific purposes or length of time for which White Castle collected, stored, used, and/or disseminated her biometric data.

48. **Prior** to the collection of her biometric identifiers and/or biometric information, Plaintiff had never been informed of any biometric retention policy developed by White Castle, nor had she ever been informed whether White Castle will ever permanently delete her biometric data.

49. **Prior** to the collection of her biometric identifiers and/or biometric information, Plaintiff had never been provided with nor ever signed a written release allowing White Castle to collect, store, use, or disseminate her biometric data.

50. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by White Castle's multiple violations of BIPA alleged herein.

51. No amount of time or money can compensate Plaintiff if her biometric data is compromised by the lax procedures through which White Castle captured, stored, used, and disseminated her and other similarly-situated individuals' biometric data. Moreover, Plaintiff would not have provided her biometric data to White Castle if she had known that it would retain such information for an indefinite period of time without her consent.

52. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act"). Nonetheless, Plaintiff has been aggrieved because she suffered an injury-in-fact based on White Castle's violations of her legal rights. White Castle intentionally interfered with Plaintiff's right to possess and control her own sensitive biometric data. Additionally, Plaintiff suffered an invasion of a legally protected interest when White Castle secured her personal and private biometric data at a time when it had no legal right to do so, a gross invasion of her right to

privacy. BIPA protects employees like Plaintiff from this precise conduct. White Castle had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

53. Plaintiff's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Plaintiff was not sufficiently compensated by White Castle for its retention and use of her and other similarly-situated employees' biometric data.

54. Plaintiff also suffered an informational injury because White Castle failed to provide her with information to which she was entitled by statute. Through BIPA, the Illinois legislature has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data: and in injury – not receiving this extremely critical information.

55. Plaintiff also suffered an injury in fact because White Castle improperly disseminated her biometric identifiers and biometric information to third parties, including Cross Match and DigitalPersona, and others that hosted the biometric data in their data centers, in violation of BIPA.

56. Pursuant to 740 ILCS 14/15(b), Plaintiff was entitled to receive certain information prior to White Castle securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which White Castle collects, stores, uses, and disseminates her biometric data; information regarding White Castle's biometric retention policy; and, a written release allowing White Castle to collect, store, use, and disseminate her private biometric data. By depriving Plaintiff of this information, White Castle injured her. *Public Citizen*

v. U.S. Department of Justice, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Atkins*, 524 U.S. 11 (1998).

57. Plaintiff has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of her biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about White Castle's policies and practices; in the form of the unauthorized disclosure of her confidential biometric data to third parties, including but not limited to Cross Match and DigitalPersona; in the form of interference with her right to control and possess her confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

58. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by White Castle. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

59. Pursuant to Rule 23(a) and 23(b) of the Federal Rules of Civil Procedure, Plaintiff brings claims on her own behalf and as representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS 14/1 *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

60. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it **first** (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time for which a

biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS § 14/15.

61. Plaintiff seeks class certification for the following class of similarly-situated individuals under BIPA:

> All individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, obtained, maintained, stored or disclosed by White Castle during the applicable statutory period.

62. This action is properly maintained as a class action under Rule 23 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiff are typical of the claims of the class; and,

D. The Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

63. The total number of putative class members exceeds 100 individuals. The exact number of class members can easily be determined from White Castle's payroll records.

Commonality

64. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, using, storing and disseminating their biometric identifiers or biometric information;

C. Whether Defendant obtained a written release (as defined in 740 ILCS § 14/10) to collect, use, store and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether Defendant has disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

F. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction with the individual, whichever occurs first;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant used Plaintiff's and the Class's fingerprints to identify them;

I. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed intentionally and/or recklessly.

65. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

66. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel that are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

67. The claims asserted by Plaintiff are typical of the class members she seeks to

represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

68. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to Rule 23(b)(3).

Predominance and Superiority

69. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

70. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and/or substantially impair or impede the ability of class members to protect their interests. The issues in

this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION
Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

71. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

72. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

73. Defendant fails to comply with these BIPA mandates.

74. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

75. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by White Castle (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

76. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

77. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

78. Upon information and belief, Defendant lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data.

79. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

80. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

81. BIPA requires companies to obtain informed written consent from employees **before** acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

82. Defendant failed to comply with these BIPA mandates.

83. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

84. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by White Castle (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

85. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

86. Defendant systematically and automatically collected, used, and stored Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

87. Prior to collecting their biometric data, Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored and used, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

88. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

89. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory

damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

90. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

91. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without **first** obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

92. Defendant fails to comply with this BIPA mandate.

93. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

94. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by White Castle (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

95. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

96. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(1).

97. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's

and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

98. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Latrina Cothron respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Latrina Cothron as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* reckless and/or intentional violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Date: April 11, 2019

Respectfully Submitted,

/s/ Andrew C. Ficzko
Ryan F. Stephan
Andrew C. Ficzko
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
aficzko@stephanzouras.com

ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on April 11, 2019, I filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

/s/ Andrew C. Ficzko